Local Decomposition of Kalman Filters and Its Application for Secure State Estimation

Xinghua Liu, Yilin Mo*, Emanuele Garone

***Abstract*—This technical note is concerned with the secure state estimation problem of a linear discrete-time Gaussian system in the presence of sparse integrity attacks. m sensors are deployed to monitor the state and p of them can potentially be compromised by an adversary, whose data can be arbitrarily manipulated by the attacker. We show that the optimal Kalman estimate can be decomposed as a weighted sum of local state estimates. Based on these local estimates, we propose a convex optimization based approach to generate a more secure state estimate. It is proved that our proposed estimator coincides with the Kalman estimator with a certain probability when all sensors are benign. Besides, we establish a sufficient condition under which the proposed estimator is stable against the (p, m)-sparse attack. A numerical example is provided to validate the secure state estimation scheme.**

***Index Terms*—Security, Kalman filter, Cyber-physical systems, Optimization.**

I. Introduction

Cyber-Physical Systems (CPS) are now playing a crucial role in many areas of modern society [1], [2], [3], [4]. The use of cyber components, though enabling more efficient design and flexible implementation, can make the CPS vulnerable to potentially devastating cyberattacks launched by insiders or resourceful foes. For example, CarShark [5], Stuxnet virus [6] and Dragonfly virus [7]. Due to the stealthiness of the attacks, system operators usually cannot discover attacks in time, which may lead to the severe economy damage and even the loss of human lives. The aforementioned incidents indicate that enhancing the security of CPS is an urgent issue. Hence, in recent years the importance of security in CPS has been acknowledged and significant efforts have been devoted into developing strategies against attacks.

In the literature, several contributions have been proposed for attack detection and attack-resilient control. Sandberg et al. [8] considered how to find a sparse stealthy input, which enables the adversary to launch an attack with a minimum number of compromised sensors. Kim et al. [9] studied a so-called framing attack that can mislead the bad data detector to mistakenly remove critical measurements, without which the network is unobservable. For a dynamical system, detecting malicious components via fault detection and isolation based methods has been extensively studied in [10]. From the viewpoint of attack-resilient control, Yuan et al. [11] proposed a coupled design framework of intrusion detection mechanisms and provided a robust control policy against DoS attacks. Ahmet et al. [12] investigated event-triggered control against jamming attacks, and presented sufficient conditions for almost sure asymptotic stabilization. For the design of state estimators, Teixeira et al. [13] analyzed the effects of possible deceptions attacks for state estimators and proposed some policies to design deception attacks for both linear and nonlinear state estimation. Qi et al. [14] considered the event-based attack strategy against remote state estimation. Recently, Mo and Sinopoli [15] proposed an estimator that has minimum mean square error against the worst-case attacks. However, the problem of designing a secure state estimator for a dynamic system is much more challenging because the bias injected by an adversary can accumulate in the dynamic state estimation and give rise to a large or even unbounded estimation error [16], [17].

To overcome the problem of bias accumulation in the dynamic state estimation, Fawzi et al. [18] proposed a moving horizon approach, where the estimator only uses the measurements from time $k - T + 1$ to time k to estimate the current state $x(k)$ and effectively reduced the dynamic state estimation problem into a static estimation problem. Pajic et al. [19], [20] further developed this approach to physical systems subject to random or bounded noise. Notice that the static estimation problem can be solved efficiently using ℓ_1 relaxation by exploiting the sparseness of the bias injected by the adversary. Shoukry et al. [21] presented a novel algorithm that uses a satisfiability modulo theory approach to harness the complexity of secure state estimation. However, the sensory data before time $k - T$ are discarded in the moving horizon approach, which may result in a degradation of the estimation performance. In view of this issue, Mo et al. [22] considered estimating state $x(k) \in \mathbb{R}^n$ from measurements subject to a (p, m)-sparse attack, and constructed a local state estimator for each sensor and the historical sensory data can be stored in the local state estimate, which is illustrated in the following Fig. 1.

Motivated by the above discussions, in this technical note, we assume the attacker can only attack up to $p < m$ sensors due to the resource limitation, and further investigate the problem of designing a secure state estimator for a linear time-invariant Gaussian system against the (p, m)-sparse attack. In contrast to the assumption in our preliminary works [22], [23], we remove a restrictive condition on the system matrices and develop a framework to implement the decomposition of Kalman filter for the more general case of linear systems. The

Xinghua Liu is with the Department of Electrical Engineering, School of Automation and Information Engineering, Xi'an University of Technology, Xi'an 710048. Email: liuxh@xaut.edu.cn

Yilin Mo is with the Department of Automation, Tsinghua University, Beijing 100084. Email: ylmo@tsinghua.edu.cn

Emanuele Garone is with the Control and System Analysis department, Universite Libre de Bruxelles, Brussels, Belgium. Email: egarone@ulb.ac.be

*Corresponding author: ylmo@tsinghua.edu.cn

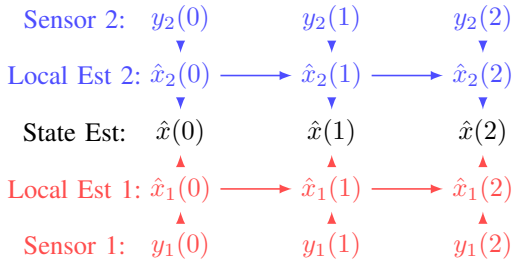

Fig. 1. The information flow of the proposed filter.

main merit of the proposed estimator design are twofold:

1) We prove that our estimator will recover the optimal Kalman estimate with a certain probability, when all sensors are benign.
2) Subject to p corrupted sensors, we provide a sufficient condition on the stability of our estimator.

The rest of this technical note is organized as follows: Section II formulates the problem formulation. In Section III, we prove that the Kalman estimator can be decomposed as a linear combination of local estimators. A convex optimization based approach is proposed in Section V to derive a secure state estimate from local estimates. The performance of the proposed estimator is illustrated via a numerical example in Section VI and finally Section VII concludes the paper.

Notation: Throughout this technical note, we adopt the following notations. For a set X, $|X|$ means the cardinal number of the set X. I is the identity matrix with suitable dimensions. The superscripts $\top$ and -1 denote matrix transposition and matrix inverse, respectively. $\mathbb{R}^n$ and $\mathbb{C}^n$ denote the set of n-dimensional real vectors and complex vectors, respectively. $\mathbb{R}^{m\times n}$ ($\mathbb{C}^{m\times n}$) is the set of all $m\times n$ real (complex) matrices. For the matrix $A\in\mathbb{C}^{m\times n}$, A^H is the conjugate transpose. $\|v\|$ is the Euclidean norm of vector v, i.e., $\|v\|=(v^\top v)^{\frac{1}{2}}$, while $\|A\|$ is spectral norm of matrix A, i.e., $\|A\|=[\lambda_{\max}(A^\top A)]^{\frac{1}{2}}$. Matrices, if their dimensions are not explicitly stated, are assumed to have compatible dimensions for algebraic operations.

II. Problem Formulation

This section formulates the secure state estimation problem for linear Gaussian system. The notation developed below is used in the remainder of this paper.

Let a linear time-invariant system

$$x(k+1)=Ax(k)+Bw(k), \tag{1}$$

where $x(k)\in\mathbb{R}^n$ is the system state at time k, $w(k)\in\mathbb{R}^s$ is the Gaussian process noise at time k, and $x(0)$ is the initial state. $w(k)$, $x(0)$ are assumed to be independent Gaussian random variables, i.e., $x(0)\sim\mathcal{N}(0,\Sigma)$, $w(k)\sim\mathcal{N}(0,Q)$. $A\in\mathbb{R}^{n\times n}$ and $B\in\mathbb{R}^{n\times s}$ are constant matrices. The following assumption is considered throughout the rest of the paper:

Assumption 1. *The matrix A is nonsingular.*

We consider that m sensors are deployed to monitor the physical system (1). The measurement from the i-th sensor at time k is:

$$y_i(k)=C_ix(k)+v_i(k)+a_i(k), \tag{2}$$

where C_i is a non-zero row vector with proper dimensions, $y_i(k)\in\mathbb{R}$ is a measurement at time k, and $v_i(k)\in\mathbb{R}$ is Gaussian measurement noise. The scalar $a_i(k)$ denotes the possible bias injected by an adversary. For a benign sensor i, $a_i(k)=0$ for all k, whereas for a compromised sensor i, $a_i(k)$ can be arbitrary. Let $\mathcal{S}=\{1,2,\cdots,m\}$ be the index set of all sensors, then a (p,m)-sparse attack is defined as follows.

Definition 1. *For an index set $\mathcal{I}\subseteq\mathcal{S}$, the complement set of $\mathcal{I}$ is denoted as $\mathcal{I}^c=\mathcal{S}\setminus\mathcal{I}$, an attack $a(k)=\left[a_1^\top(k)\ \cdots\ a_m^\top(k)\right]^\top$ is called the (p,m)-sparse attack if the following conditions are satisfied: (i) $\|a_i(k)\|=0$, $\forall i\in\mathcal{I}^c$; (ii) $|\mathcal{I}|\leq p$.*

We further assume that the set of compromised sensors remains fixed over time. Define the collection of all possible index sets of malicious sensors as $\mathcal{C}\triangleq\{\mathcal{I}:\mathcal{I}\subseteq\mathcal{S},|\mathcal{I}|=p\}$.

By defining the aggregated vectors

$$\begin{aligned} y(k)&\triangleq\left[y_1^\top(k)\quad\cdots\quad y_m^\top(k)\right]^\top,\\ C&\triangleq\left[C_1^\top\quad\cdots\quad C_m^\top\right]^\top,\\ v(k)&\triangleq\left[v_1^\top(k)\cdots v_m^\top(k)\right]^\top, \end{aligned} \tag{3}$$

we can rewrite (2) as

$$y(k)=Cx(k)+v(k)+a(k). \tag{4}$$

where $v(k)\in\mathbb{R}^m$ is a vector of measurement noise. It is assumed that $v(k)\sim\mathcal{N}(0,R)$ with $R>0$ is i.i.d and independent of the noise process $\{w(k)\}$ and the initial condition $x(0)$. Without loss of generality, in this note we assume (A,C) to be observable. In the case where (A,C) is not observable, we can always perform a Kalman decomposition and consider only the observable space.

If all sensors are benign, i.e., $a(k)=0$ for all k, the optimal state estimator is the classical Kalman filter:

$$\begin{aligned} \hat{x}(k)&=\hat{x}(k|k-1)+K(k)\left[y(k)-C\hat{x}(k|k-1)\right],\\ P(k)&=P(k|k-1)-K(k)CP(k|k-1), \end{aligned}$$

where

$$\begin{aligned} &\hat{x}(k+1|k)=A\hat{x}(k),\\ &P(k+1|k)=AP(k)A^\top+BQB^\top,\\ &K(k)=P(k|k-1)C^\top(CP(k|k-1)C^\top+R)^{-1}, \end{aligned}$$

with initial condition $\hat{x}(0|-1)=0$, $P(0|-1)=\Sigma$.

Since the system is observable, according to [24], it is well known that the estimation error covariance matrices $P(k)$ and the gain $K(k)$ will converge to

$$P\triangleq\lim_{k\to\infty}P(k),\quad P_+=APA^\top+BQB^\top, \tag{5}$$

$$K\triangleq P_+C^\top(CP_+C^\top+R)^{-1}. \tag{6}$$

Since typically the control system will be running for an extended period of time, we can assume that the Kalman filter

is at steady state, or equivalently that $\Sigma = P$. Thus the Kalman filter reduces to the following fixed-gain linear estimator:

$$\hat{x}(k+1) = (A - KCA)\hat{x}(k) + Ky(k+1). \tag{7}$$

We denote the matrix $K = [K_1, \ldots, K_m]$, where K_i stands for the ith column vector of K. Accordingly, (7) can be rewritten as

$$\hat{x}(k+1) = (A - KCA)\hat{x}(k) + \sum_{i=1}^{m} K_i y_i(k+1). \tag{8}$$

The goal of this paper is to design a estimation algorithm such that: if $a_i(k) = 0$ for all k and i, the estimate coincides with the Kalman estimate as described by (7) with a certain probability; if p sensors are compromised, it still gives a stable estimate against the (p, m)-sparse attack. To achieve this objective, in this paper we will first propose an approach to decompose the Kalman estimate into a linear combination of estimates generated by a set of local estimators. Then, a secure fusion scheme is presented to replace the linear fusion scheme.

III. Decomposition of Kalman Filter using Local Estimate

In this section, we propose a method to decompose the Kalman estimate (7) into a weighted sum of the local state estimates $\hat{\zeta}_i(k)$, $i = 1, \ldots, m$, which leverage on all the historical measurements and reduce the computational burden of the central estimator. We further assume the following condition through the rest of the paper:

Assumption 2. *[22] The matrix $A - KCA$ and matrix A do not share any eigenvalue.*

The matrix $A - KCA$ can be decomposed into a Jordan form, i.e.,

$$A - KCA = \mathcal{V}\mathcal{J}\mathcal{V}^{-1}. \tag{9}$$

where $\mathcal{J} = \text{diag}\{J_1, J_2, \cdots, J_p\}$, each Jordan block $J_l \in \mathbb{C}^{n_l \times n_l}$ with eigenvalue λ_l is

$$J_l = \begin{bmatrix} \lambda_l & 1 & & & 0 \\ & \lambda_l & 1 & & \\ & & \ddots & \ddots & \\ & 0 & & \ddots & 1 \\ & & & & \lambda_l \end{bmatrix},$$

and $\sum_{l=1}^{p} n_i = n$ for $l = 1, 2, \cdots, p$.

Define $\mathcal{Q} = \mathcal{V}^{-1} = [Q_1^H, \cdots, Q_p^H]^H$ and $Q_l^H = \begin{bmatrix} \alpha_{l,1} & \cdots & \alpha_{l,n_l} \end{bmatrix}$, where $\alpha_{l,1} \in \mathbb{C}^n, \cdots, \alpha_{l,n_l} \in \mathbb{C}^n$, and $Q_l \in \mathbb{C}^{n_l \times n}$ for $l = 1, 2, \cdots, p$. We can rewrite (8) as

$$\mathcal{Q}\hat{x}(k+1) = \mathcal{J}\left[\mathcal{Q}\hat{x}(k)\right] + \sum_{i=1}^{m} \mathcal{Q}K_i y_i(k+1). \tag{10}$$

Unlike our preliminary paper [22] which requires the observability of the system from each sensor, in this technical note, we deal with the general case that the system is not necessarily fully observable by the ith sensor, i.e., (A, C_i) may not be observable. At this point, our goal is to generate m local state estimates $\hat{\zeta}_i(k)$, $i = 1, \ldots, m$, such that:

1) Each local estimator generates a stable estimate on the subspace that is observable to the sensor;
2) The Kalman estimate $\hat{x}(k)$ can be recovered as a linear combination of $\hat{\zeta}_i(k)$, i.e.,

$$\hat{x}(k) = \mathcal{F}_1\hat{\zeta}_1(k) + \ldots + \mathcal{F}_m\hat{\zeta}_m(k). \tag{11}$$

Remark 1. *The core of this decomposition is that (11) will be interpreted as the solution of a least square problem in the next section. The coefficients of least square fusion are time-invariant. Under **Assumption 1** and **Assumption 2**, we are able to obtain a particular decomposition based on the algebraic analysis to guarantee the convergence and uniqueness of the least square fusion coefficients.*

Assuming that the local estimates are computed as

$$\hat{\zeta}_i(k+1) = \mathcal{J}\hat{\zeta}_i(k) + \mathbf{1}_n y_i(k+1), \quad \zeta_i(0) = 0, \tag{12}$$

where $\mathbf{1}_n \in \mathbb{R}^{n \times 1}$ is an all-one vector and $\mathcal{J}$ is defined in (9), the following result can be proved.

Theorem 1. *The state estimate $\hat{x}$ obtained using (11)-(12) coincides with the Kalman state estimator (7) under the condition that $\mathcal{F}_i$ is selected as*

$$\mathcal{F}_i = \mathcal{V}\mathcal{X}_i, \tag{13a}$$
$$\mathcal{X}_i = \text{diag}\{X_{1,i}, X_{2,i}, \cdots, X_{p,i}\}. \tag{13b}$$

and $X_{l,i}$ is

$$X_{l,i} = \begin{bmatrix} x_{n_l,i} & x_{n_l-1,i} & \cdots & x_{2,i} & x_{1,i} \\ & x_{n_l,i} & \ddots & x_{3,i} & x_{2,i} \\ & & x_{n_l,i} & \ddots & \vdots \\ & 0 & & x_{n_l,i} & x_{n_l-1,i} \\ & & & & x_{n_l,i} \end{bmatrix}, \tag{14}$$

where $l = 1, 2, \cdots, p$ and

$$x_{n_l,i} = \alpha_{l,n_l}^H K_i,\ x_{n_l-1,i} = (\alpha_{l,n_l-1}^H - \alpha_{l,n_l}^H)K_i,$$
$$\cdots\cdots,\ x_{2,i} = (\alpha_{l,2}^H - \alpha_{l,3}^H)K_i,\ x_{1,i} = (\alpha_{l,1}^H - \alpha_{l,2}^H)K_i.$$

Proof: According to the form of (13b) and (14), it can be verified that:

$$\mathcal{X}_i\mathbf{1}_n = \begin{bmatrix} \alpha_{1,1}^H K_i \\ \vdots \\ \alpha_{1,n_1}^H K_i \\ \vdots \\ \alpha_{p,1}^H K_i \\ \vdots \\ \alpha_{p,n_p}^H K_i \end{bmatrix} = \begin{bmatrix} Q_1 \\ Q_2 \\ \vdots \\ Q_p \end{bmatrix} K_i = \mathcal{Q}K_i. \tag{15}$$

Since $\mathcal{X}_i$ and $\mathcal{J}$ are block diagonal matrices with appropriate dimensions, we obtain that

$$\mathcal{X}_i\mathcal{J} = \mathcal{J}\mathcal{X}_i. \tag{16}$$

Therefore, multiplying both sides of (12) by $\mathcal{V}\mathcal{X}_i$, we obtain

$$\begin{aligned}\mathcal{V}\mathcal{X}_i\hat{\zeta}_i(k+1) &= \mathcal{V}\mathcal{X}_i\mathcal{J}\hat{\zeta}_i(k) + \mathcal{V}\mathcal{X}_i\mathbf{1}_n y_i(k+1)\\ &= \mathcal{V}\mathcal{J}\mathcal{V}^{-1}\mathcal{V}\mathcal{X}_i\hat{\zeta}_i(k) + K_i y_i(k+1)\\ &= (A-KCA)\mathcal{V}\mathcal{X}_i\hat{\zeta}_i(k) + K_i y_i(k+1). \quad (17)\end{aligned}$$

Comparing (8) and (17), we can obtain the decomposition (11) with $\mathcal{F}_i = \mathcal{V}\mathcal{X}_i$. ∎

To study the relationship between the local estimate $\hat{\zeta}_i(k)$ and the state $x(k)$, define the matrices $\mathcal{G}_i = \begin{bmatrix}G_{1,i}^H & G_{2,i}^H & \cdots & G_{p,i}^H\end{bmatrix}^H \in \mathbb{C}^{n\times n}$ for $i = 1, 2, \cdots, m$, where

$$G_{l,i} = \begin{bmatrix} C_iA(A-\lambda_l I)^{-n_l} + \cdots + C_iA(A-\lambda_l I)^{-1} \\ \vdots \\ C_iA(A-\lambda_l I)^{-2} + C_iA(A-\lambda_l I)^{-1} \\ C_iA(A-\lambda_l I)^{-1}\end{bmatrix}_{n_l\times n} \quad (18)$$

for $l = 1, 2, \cdots, p$. Note that the inverse of $A - \lambda_i I$ is well defined since A does not share eigenvalues with $A - KCA$ and $\mathcal{J}$. The following corollary can be proved.

Corollary 1. *Let $\epsilon_i(k) \triangleq \mathcal{G}_i x(k) - \hat{\zeta}_i(k)$, then*

$$\begin{aligned}\epsilon_i(k+1) = \mathcal{J}\epsilon_i(k) + (\mathcal{G}_iB - \mathbf{1}_nC_iB)w(k)\\ - \mathbf{1}_n v_i(k+1) - \mathbf{1}_n a_i(k+1). \quad (19)\end{aligned}$$

In other words, $\hat{\zeta}_i(k)$ is a stable estimate of $\mathcal{G}_i x(k)$ since $A - KCA$ is stable.

Proof: By the definition of $\epsilon_i(k)$, we have

$$\begin{aligned}\epsilon_i(k+1) &= \mathcal{G}_i x(k+1) - \hat{\zeta}_i(k+1)\\ &= (\mathcal{G}_iA - \mathbf{1}_nC_iA)x(k) - \mathcal{J}\hat{\zeta}_i(k)\\ &\quad + (\mathcal{G}_iB - \mathbf{1}_nC_iB)w(k) - \mathbf{1}_n v_i(k+1) - \mathbf{1}_n a_i(k+1).\end{aligned}$$

Furthermore, it can be verified that $G_{l,i}A - \mathbf{1}_{n_l}C_iA = J_lG_{l,i}$. These two facts imply that

$$\mathcal{G}_iA - \mathbf{1}_nC_iA = \mathcal{J}\mathcal{G}_i. \quad (20)$$

Therefore, we obtain that

$$\begin{aligned}\epsilon_i(k+1) = \mathcal{J}\epsilon_i(k) + (\mathcal{G}_iB - \mathbf{1}_nC_iB)w(k)\\ - \mathbf{1}_n v_i(k+1) - \mathbf{1}_n a_i(k+1),\end{aligned}$$

which concludes the proof. ∎

The following lemma is proposed to characterize a further interesting property of $\mathcal{F}_i$ and $\mathcal{G}_i$, for $i = 1, 2, \cdots, m$.

Lemma 1. *Under Assumption 1, the matrices $\mathcal{F}_1, \cdots, \mathcal{F}_m$ and matrices $\mathcal{G}_1, \cdots, \mathcal{G}_m$ satisfy the following equation:*

$$\sum_{i=1}^m \mathcal{F}_i\mathcal{G}_i = I. \quad (21)$$

Proof: According to (13a), it follows that

$$\mathcal{F}_i\mathcal{G}_i = \mathcal{V}\mathcal{X}_i\mathcal{G}_i = \mathcal{V}\begin{bmatrix}X_{1,i}G_{1,i}\\ \vdots \\ X_{p,i}G_{p,i}\end{bmatrix}.$$

Considering $\sum_{i=1}^m X_{l,i}G_{l,i},\ \forall l = 1, 2, \cdots, p$, we obtain the following equation

$$\sum_{i=1}^m X_{l,i}G_{l,i} = \sum_{i=1}^m \begin{bmatrix} \sum_{h=1}^{n_l}\alpha_{l,h}^H K_iC_iA(A-\lambda_l I)^{-h} \\ \sum_{h=2}^{n_l}\alpha_{l,h}^H K_iC_iA(A-\lambda_l I)^{1-h} \\ \vdots \\ \sum_{h=n_l-1}^{n_l}\alpha_{l,h}^H K_iC_iA(A-\lambda_l I)^{(n_l-2)-h} \\ \alpha_{l,n_l}^H K_iC_iA(A-\lambda_l I)^{-1}\end{bmatrix}. \quad (22)$$

Since $Q_l(A - KCA) = J_lQ_l$, we have that

$$\begin{aligned}&\alpha_{l,n_l}^H KCA = \alpha_{l,n_l}^H(A-\lambda_l I),\\ &\alpha_{l,n_l-1}^H KCA = \alpha_{l,n_l-1}^H(A-\lambda_l I) - \alpha_{l,n_l}^H,\\ &\qquad\vdots\\ &\alpha_{l,1}^H KCA = \alpha_{l,1}^H(A-\lambda_l I) - \alpha_{l,2}^H. \quad (23)\end{aligned}$$

By noticing that $\sum_{i=1}^m K_iC_i = KC$ and substituting (23) into (22), then we can obtain that

$$\sum_{i=1}^m X_{l,i}G_{l,i} = \begin{bmatrix}\alpha_{l,1} & \cdots & \alpha_{l,n_l}\end{bmatrix}^H = Q_l.$$

Finally, we have

$$\sum_{i=1}^m \mathcal{F}_i\mathcal{G}_i = \mathcal{V}\begin{bmatrix}\sum_{i=1}^m X_{1,i}G_{1,i}\\ \vdots \\ \sum_{i=1}^m X_{p,i}G_{p,i}\end{bmatrix} = \mathcal{V}\begin{bmatrix}Q_1\\ \vdots \\ Q_p\end{bmatrix} = \mathcal{V}\mathcal{Q} = I.$$

∎

IV. A LEAST SQUARE INTERPRETATION FOR THE DECOMPOSITION

In this section, we show that the linear fusion scheme (11) can be interpreted as the solution of a least square problem, which will be used later to derive a secure fusion scheme.

According to the recursive equation (19), let $\epsilon_i(k) = \phi_i(k) + \varphi_i(k)$ and define $\phi_i(k), \varphi_i(k)$ as follows:

$$\begin{aligned}&\phi_i(k+1) = \mathcal{J}\phi_i(k) + (\mathcal{G}_iB - \mathbf{1}_nC_iB)w(k) - \mathbf{1}_n v_i(k+1),\\ &\varphi_i(k+1) = \mathcal{J}\varphi_i(k) - \mathbf{1}_n a_i(k+1). \quad (24)\end{aligned}$$

where $\phi_i(k)$ can be regarded as the error of the local estimate caused by the noise and $\varphi_i(k)$ as the error caused by the bias injected by the adversary.

Furthermore, denote $\widetilde{\mathcal{J}} \in \mathbb{C}^{mn\times mn}$, $\tilde{\phi}(k) \in \mathbb{C}^{mn}$, $\tilde{\varphi}(k) \in \mathbb{C}^{mn}$, $\tilde{\epsilon}(k) \in \mathbb{C}^{mn}$ as

$$\begin{aligned}&\widetilde{\mathcal{J}} \triangleq \mathrm{diag}\{\mathcal{J}, \cdots, \mathcal{J}\},\ \tilde{\phi}(k) \triangleq \begin{bmatrix}\phi_1^H(k) & \cdots & \phi_m^H(k)\end{bmatrix}^H,\\ &\tilde{\varphi}(k) \triangleq \begin{bmatrix}\varphi_1^H(k) \cdots \varphi_m^H(k)\end{bmatrix}^H,\ \tilde{\epsilon}(k) \triangleq \begin{bmatrix}\epsilon_1^H(k) \cdots \epsilon_m^H(k)\end{bmatrix}^H. \quad (25)\end{aligned}$$

Following the property of linear transformation from Gaussian random vectors, we know that $\tilde{\phi}(k)$ will be Gaussian distributed and its covariance satisfies the following Lyapunov equation:

$$\mathrm{Cov}[\tilde{\phi}(k+1)] = \widetilde{\mathcal{J}}\,\mathrm{Cov}[\tilde{\phi}(k)]\widetilde{\mathcal{J}}^H + \Xi. \quad (26)$$

where $\Xi = \Xi_1 + \Xi_2$ and

$$\Xi_1 = \mathrm{Cov}\left[\begin{pmatrix} \mathcal{G}_1 B - \mathbf{1}_n C_1 B \\ \vdots \\ \mathcal{G}_m B - \mathbf{1}_n C_m B \end{pmatrix} w(k)\right] = \begin{bmatrix} \mathcal{G}_1 B - \mathbf{1}_n C_1 B \\ \vdots \\ \mathcal{G}_m B - \mathbf{1}_n C_m B \end{bmatrix} Q \begin{bmatrix} \mathcal{G}_1 B - \mathbf{1}_n C_1 B \\ \vdots \\ \mathcal{G}_m B - \mathbf{1}_n C_m B \end{bmatrix}^H, \quad (27)$$

$$\Xi_2 = \mathrm{Cov}\left[\begin{pmatrix} \mathbf{1}_n v_1(k+1) \\ \vdots \\ \mathbf{1}_n v_m(k+1) \end{pmatrix}\right] = \mathbf{1}_{mn\times mn} \circ (R \otimes \mathbf{1}_{n\times n}). \quad (28)$$

where $\circ$ denotes element-wise matrix multiplication, $\otimes$ is the Kronecker product, and $\mathbf{1}_{mn\times mn}$ is an all one matrix of size $mn \times mn$.

Define $\widetilde{\mathcal{W}}$ as the fix point[1] of (26), i.e.,

$$\widetilde{\mathcal{W}} = \widetilde{\mathcal{J}}\widetilde{\mathcal{W}}\widetilde{\mathcal{J}}^H + \Xi. \quad (29)$$

Now, we propose the following optimization problem:

$$\begin{aligned} \underset{\check{x}(k),\check{\epsilon}(k)}{\text{minimize}} \quad & \frac{1}{2}\check{\epsilon}(k)^H \widetilde{\mathcal{W}}^{-1}\check{\epsilon}(k) \\ \text{subject to} \quad & \begin{bmatrix} \hat{\zeta}_1(k) \\ \vdots \\ \hat{\zeta}_m(k) \end{bmatrix} = \begin{bmatrix} \mathcal{G}_1 \\ \vdots \\ \mathcal{G}_m \end{bmatrix} \check{x}(k) - \check{\epsilon}(k). \end{aligned} \quad (30)$$

This problem can be interpreted as the problem of finding an estimate $\check{x}(k)$ that minimizes a weighted least square of the error with the local estimates $\hat{\zeta}_i(k)$, where the weighting matrix is related with the covariance of the error of the local estimates.

We are now ready to establish the connection between the linear fusion scheme (11) and the least-square problem (30), which is developed in the following theorem.

Theorem 2. *The solution of the least-square problem* (30) *is*

$$\check{x}(k) = \sum_{i=1}^{m} \mathcal{F}_i \hat{\zeta}_i(k) = \hat{x}(k),$$
$$\check{\epsilon}(k) = \left(I - \begin{bmatrix} \mathcal{G}_1 \\ \vdots \\ \mathcal{G}_m \end{bmatrix} \begin{bmatrix} \mathcal{F}_1 & \dots & \mathcal{F}_m \end{bmatrix}\right) \tilde{\epsilon}(k).$$

Proof: For the sake of legibility, the proof is reported in the Appendix A. ∎

Remark 2. *It should be noticed that the framework can be easily generalized to decompose other linear fixed-gain estimators, e.g., H_2 and H_∞ estimators, since the proof technique presented in* ***Theorem*** *2 is purely algebraic.*

We know that the linear fusion scheme (11) is not secure in the sense that if sensor i is compromised, then the adversary can manipulate $\hat{\zeta}_i(k)$ by injecting the bias $a_i(k)$ into the measurements $y_i(k)$. Therefore, the adversary can potentially change the Kalman estimate arbitrarily. To crack the security challenges, in Section V, we modify (30) by adding an ℓ_1 penalty to guarantee the stability of the state estimation in the presence of malicious sensors.

[1] $\widetilde{\mathcal{W}}$ is well defined since the Jordan form $\mathcal{J}$ is strictly stable

V. A Secure Information Fusion Scheme

In this section, we consider two scenarios of attack model and propose a convex optimization approach to combine the local estimate into a more secure state estimate.

Notice that the error $\epsilon_i(k)$ can be decomposed as the error $\phi_i(k)$ caused by the noise and the error $\varphi_i(k)$ caused by the bias injected by the adversary. As a result, we propose the following secure fusion scheme based on LASSO [25]:

$$\begin{aligned} \underset{\check{x}_s(k),\check{\phi}(k),\check{\varphi}(k)}{\text{minimize}} \quad & \frac{1}{2}\check{\phi}(k)^H \widetilde{\mathcal{W}}^{-1}\check{\phi}(k) + \gamma\|\check{\varphi}(k)\|_1 \\ \text{subject to} \quad & \hat{\zeta}_i(k) = \mathcal{G}_i\check{x}_s(k) - \check{\phi}_i(k) - \check{\varphi}_i(k),\ \forall i \in \mathcal{S}, \end{aligned} \quad (31)$$

where $\check{x}_s(k)$ is the secure state estimation, γ is a constant chosen by the system operator, and $\check{\phi}(k)$, $\check{\varphi}(k)$ are defined as:

$$\check{\phi}(k) \triangleq \begin{bmatrix} \check{\phi}_1(k) \\ \vdots \\ \check{\phi}_m(k) \end{bmatrix}, \ \check{\varphi}(k) \triangleq \begin{bmatrix} \check{\varphi}_1(k) \\ \vdots \\ \check{\varphi}_m(k) \end{bmatrix}.$$

We now consider two scenarios: i) all sensors are benign and the system is operating normally; ii) p sensors are compromised. The following two theorems characterize the performance of the secure fusion scheme (31) for each scenario:

Theorem 3. *Let $\check{x}_s(k)$, $\check{\phi}(k)$, $\check{\varphi}(k)$ be the minimizer for the optimization problem* (31)*. Let $\check{x}(k), \check{\epsilon}(k)$ be the minimizer for the least-square problem* (30)*. Then the following statements hold:*

1) *The following inequality holds:*

$$\|\widetilde{\mathcal{W}}^{-1}\check{\phi}(k)\|_\infty \le \gamma. \quad (32)$$

2) *Suppose that all the sensors are benign, i.e., $a(k) = 0$ for all k. We conclude that $\check{x}_s(k) = \check{x}(k) = \hat{x}(k)$, $\check{\phi}(k) = \check{\epsilon}(k)$, $\check{\varphi}(k) = 0$, if the following inequality holds:*

$$\left\| \widetilde{\mathcal{W}}^{-1} \left(I - \begin{bmatrix} \mathcal{G}_1 \\ \vdots \\ \mathcal{G}_m \end{bmatrix} \begin{bmatrix} \mathcal{F}_1 & \dots & \mathcal{F}_m \end{bmatrix}\right) \tilde{\epsilon}(k) \right\|_\infty \le \gamma. \quad (33)$$

Proof: The proof easily follows from [22], hence we omit it here to save the space. ∎

Remark 3. *If the system is operating long enough and all sensors are benign, we have $\mathrm{Cov}(\tilde{\epsilon}(k)) \approx \tilde{W}$ and we can compute the probability that the secure state estimate equals to the optimal Kalman estimate.*

For the second scenario, we consider p ($p < m$) sensors are compromised. The stability of the proposed secure estimator is characterized by the following theorem.

Theorem 4. *Suppose that p $(p < m)$ sensors are compromised, then the secure state estimate $\check{x}_s(k)$ is stable against the (p, m)-sparse attack if the following inequality holds for all $u \neq 0$:*

$$\sum_{i\in\mathcal{I}} \|\mathcal{G}_i u\|_1 < \sum_{i\in\mathcal{I}^c} \|\mathcal{G}_i u\|_1, \quad \forall \mathcal{I} \in \mathcal{C}.$$

Proof: The proof directly follows from Theorem 2 in [26]. ■

VI. Numerical Example

In this section, we demonstrate our proposed secure estimation via a numerical example. We assume the following matrix parameters for the system (1) and (4):

$$A = \text{diag}\{1, 1, -2\}, \quad B = I_3, \quad Q = I_3,$$
$$C = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & -1 \\ 1 & 2 & 1 \\ 1 & -1 & -0.5 \\ -0.5 & 1 & 1 \end{bmatrix}, \quad R = I_5.$$

One can verify that the system is not fully observable by the first sensor.

The optimal steady state Kalman gain matrix K and estimation covariance matrix P are

$$K = \begin{bmatrix} 0.2443 & 0.0431 & 0.1942 & 0.2693 & -0.0885 \\ -0.0838 & 0.2494 & 0.1469 & -0.1991 & 0.0846 \\ 0.1175 & -0.4272 & 0.2265 & 0.0629 & 0.1955 \end{bmatrix},$$
$$P = \begin{bmatrix} 0.2443 & -0.0838 & 0.1175 \\ -0.0838 & 0.1879 & -0.1452 \\ 0.1175 & -0.1452 & 0.3995 \end{bmatrix}. \tag{34}$$

The corresponding matrix $A - KCA$ has eigenvalues at 0.1061, 0.1925 and -0.2848. As a result, we can derive the matrices $\mathcal{G}_i$ as follows:

$$\mathcal{G}_1 = \begin{bmatrix} 0.7783 & 0 & 0 \\ 1.1187 & 0 & 0 \\ 1.2384 & 0 & 0 \end{bmatrix}, \mathcal{G}_2 = \begin{bmatrix} 0.7783 & 0.7783 & -1.1660 \\ 1.1187 & 1.1187 & -0.9496 \\ 1.2384 & 1.2384 & -0.9122 \end{bmatrix},$$
$$\mathcal{G}_3 = \begin{bmatrix} 0.7783 & 1.5567 & 1.1660 \\ 1.1187 & 2.2373 & 0.9496 \\ 1.2384 & 2.4768 & 0.9122 \end{bmatrix},$$
$$\mathcal{G}_4 = \begin{bmatrix} 0.7783 & -0.7783 & -0.5830 \\ 1.1187 & -1.1187 & -0.4748 \\ 1.2384 & -1.2384 & -0.4561 \end{bmatrix},$$
$$\mathcal{G}_5 = \begin{bmatrix} -0.3892 & 0.7783 & 1.1660 \\ -0.5593 & 1.1187 & 0.9496 \\ -0.6192 & 1.2384 & 0.9122 \end{bmatrix}.$$

We consider two scenarios: i) all sensors are benign; ii) the first sensor is under attack and $a_1(k) = 100$ for all k. Define the empirical Mean Squared Error (MSE) as

$$\text{MSE} = \frac{\sum_{k=1}^{T} \|\check{x}_s(k) - x(k)\|^2}{T},$$

where T denotes iterative steps of the time. We then compute MSE of the secure estimator for each scenario with different choices of γ.

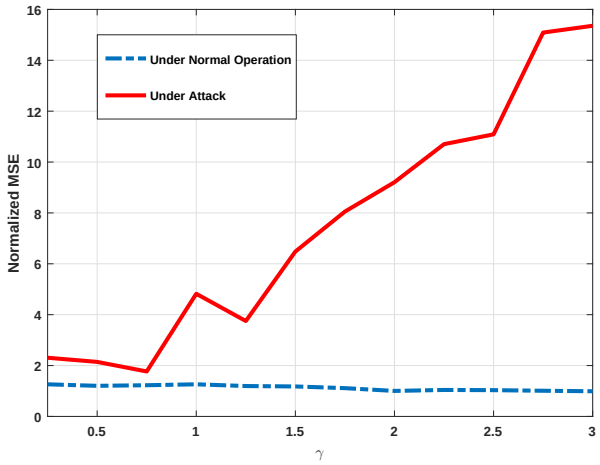

Fig. 2. Normalized MSE of the secure estimator v.s. different choices of γ.

When all sensors are benign, the optimal Kalman estimator has an MSE equals to $\text{tr}(P)$. In our simulation, $\text{tr}(P) = 0.8317$. Hence, we define the normalized MSE as the MSE divided by 0.8317. Fig. 2 illustrates the normalized MSE of the proposed secure estimator versus γ. It can be seen that when $\gamma \geq 2$, the secure estimator achieves roughly the same estimation performance as the optimal Kalman estimator under normal operation. On the other hand, if sensor 1 is malicious, then the MSE achieves the minimum at around $\gamma = 0.75$.

Remark 4. ***Theorem 3*** *indicates that increasing γ will increase the likelihood that the secure estimation equals the Kalman estimation during normal operation, then we can see that the estimation performance under normal operation is better with a larger γ in Fig. 2. On the other hand, the larger γ may cause performance degradation under attack. However, we can see that there is an optimal γ for the estimation performance under attack. Hence, in practice we can adjust the parameter γ to obtain a desirable tradeoff between different scenarios.*

VII. Conclusion

In this technical note, the problem of secure state estimation has been investigated for a linear time-invariant Gaussian system in the presence of sparse integrity attacks. The system may be unobservable by some sensors and p of m sensors can potentially be compromised by an adversary. We establish a framework to generate the local state estimate and achieve the decomposition of Kalman filter, which coincides with a certain probability to the Kalman estimate when the system is under normal operation. Using convex optimization, we combine the local estimate into a more secure state estimate and propose a sufficient condition under which the secure state estimator is stable against the (p, m)-sparse attack. A numerical example with simulation results has shown a good performance of the proposed secure estimator. In the future, we will consider how to perform the Kalman filter decomposition and how to design secure state estimate for the time-varying systems.

APPENDIX A
PROOF OF THEOREM 2

In order to prove Theorem 2, we need two preliminary lemmas.

Lemma 2. *Let K be the steady state Kalman gain defined in* (6)*. For any matrix L, such that $A-LCA$ is strictly stable, then we have that*

$$P = (A-KCA)P(A-LCA)^H + (B-KCB)Q(B-LCB)^H + KRL^H, \quad (35)$$

where P is defined in (5)*.*

Proof: The proof is omitted here, since it easily follows from [22]. ∎

Lemma 3. *Denote the covariance matrix $R=[r_{ij}]_{m\times m}$, for $i,j=1,2,\cdots,m$, the following Lyapunov equation holds:*

$$P\mathcal{G}_j^H = (A-KCA)P\mathcal{G}_j^H\mathcal{J} + (B-KCB)Q \times (\mathcal{G}_jB - \mathbf{1}_nC_jB)^H + \sum_{i=1}^m r_{ij}K_i\mathbf{1}_n^H, \quad (36)$$

where P is defined in (5)*.*

Proof: Define the matrix $\mathcal{L}_j \in \mathbb{C}^{n\times m}$ as an all zero matrix except that the jth column is $L_j \in \mathbb{C}^n$, i.e.,

$$\mathcal{L}_j = \begin{bmatrix}0 & \cdots & 0 & L_j & 0 & \cdots & 0\end{bmatrix},$$

where L_j satisfies the assumption in Lemma 2, i.e., $A-L_jCA$ is strictly stable.

It can be verified that

$$\mathcal{L}_jC = L_jC_j,\ KR\mathcal{L}_j^H = \sum_{i=1}^m r_{ij}K_iL_j^H.$$

According to Lemma 2, we can rewrite (35) into the following form:

$$P = (A-KCA)P(A-L_jC_jA)^H + (B-KCB)Q(B-L_jC_jB)^H + \sum_{i=1}^m r_{ij}K_iL_j^H, \quad (37)$$

which satisfies for any $L_j \in \mathbb{C}^n$.

Here we choose $L_{o,l,j} \in \mathbb{C}^{n\times 1}$ such that $L_{o,l,j}^H G_{o,l,j}^H = 1$, where $o=1,2,\cdots,n_l$, $l=1,2,\cdots,p$ and $G_{o,l,j}$ represents the oth row of matrix $G_{l,j}$ described in (18). Since C_i is a non-zero row vector and $A-\lambda_lI$ is invertible, $G_{o,l,j}$ is a non-zero row vector for all $o=1,2,\cdots,n_l$, $l=1,2,\cdots,p$. Thus we can always find a column vector $L_{o,l,j}$ to satisfy the condition $G_{o,l,j}L_{o,l,j}=1$.

Right multiplying $G_{o,l,j}^H$ at the RHS and LHS of (37), we can obtain that

$$PG_{o,l,j}^H = (A-KCA)P(A^HG_{o,l,j}^H - A^TC_j^H) + (B-KCB)Q(B^HG_{o,l,j}^H - B^HC_j^H) + \sum_{i=1}^m r_{ij}K_i. \quad (38)$$

Since $G_{l,j}^H = [G_{1,l,j}^H \ \cdots\ G_{o,l,j}^H \ \cdots\ G_{n_l,l,j}^H]$, we can rewrite (38) in the following form:

$$PG_{l,j}^H = (A-KCA)P(A^HG_{l,j}^H - A^TC_j^H\mathbf{1}_{n_l}^H) + (B-KCB)Q(G_{l,j}B - \mathbf{1}_{n_l}C_jB)^H + \sum_{i=1}^m r_{ij}K_i\mathbf{1}_{n_l}^H.$$

Due to $\mathcal{G}_j^H = [G_{1,j}^H \ \cdots\ G_{l,j}^H \ \cdots\ G_{p,j}^H]$ and (20), it follows that

$$\begin{aligned}P\mathcal{G}_j^H &= (A-KCA)P(A^H\mathcal{G}_j^H - A^HC_j^H\mathbf{1}_n^H) + (B-KCB)Q(\mathcal{G}_jB - \mathbf{1}_nC_jB)^H + \sum_{i=1}^m r_{ij}K_i\mathbf{1}_n^H \\ &= (A-KCA)P\mathcal{G}_j^H\mathcal{J} + (B-KCB)Q \times (\mathcal{G}_jB - \mathbf{1}_nC_jB)^H + \sum_{i=1}^m r_{ij}K_i\mathbf{1}_n^H.\end{aligned}$$

∎

Proof of Theorem 2: We rewrite the matrix $\widetilde{\mathcal{W}}$ in a block diagonal form:

$$\widetilde{\mathcal{W}} = \begin{bmatrix}\widetilde{W}_{11} & \cdots & \widetilde{W}_{1m}\\ \vdots & \ddots & \vdots \\ \widetilde{W}_{m1} & \cdots & \widetilde{W}_{mm}\end{bmatrix},$$

where each $\widetilde{W}_{ij} \in \mathbb{C}^{n\times n}$. As a result, by (29), we know that $\widetilde{W}_{ij}$ satisfies:

$$\widetilde{W}_{ij} = \mathcal{J}\widetilde{W}_{ij}\mathcal{J} + (\mathcal{G}_iB - \mathbf{1}_nC_iB)Q(\mathcal{G}_jB - \mathbf{1}_nC_jB)^H + r_{ij}\mathbf{1}_n\mathbf{1}_n^H. \quad (39)$$

According to (13a), (15) and (16), we know that

$$\begin{aligned}\mathcal{F}_i\mathcal{J} &= \mathcal{V}\mathcal{X}_i\mathcal{J} = \mathcal{V}\mathcal{J}\mathcal{X}_i = \mathcal{V}\mathcal{J}\mathcal{V}^{-1}\mathcal{V}\mathcal{X}_i \\ &= \mathcal{V}\mathcal{J}\mathcal{V}^{-1}K_i = (A-KCA)F_i, \\ \mathcal{F}_i\mathbf{1}_n &= \mathcal{V}\mathcal{X}_i\mathbf{1}_n = \mathcal{V}\mathcal{Q}K_i = K_i.\end{aligned}$$

Left multiplying $\mathcal{F}_i$ at the RHS and LHS of (39), we deduce that

$$\mathcal{F}_i\widetilde{W}_{ij} = (A-KCA)\mathcal{F}_i\widetilde{W}_{ij}\mathcal{J} + (\mathcal{F}_i\mathcal{G}_iB - K_iC_iB) \times Q(\mathcal{G}_jB - \mathbf{1}_nC_jB)^H + r_{ij}K_i\mathbf{1}_n^H.$$

Therefore, let $\widetilde{\mathcal{S}}_j = \sum_{i=1}^m \mathcal{F}_i\widetilde{W}_{i,j}$, by *Lemma 1* and $\sum_{i=1}^m(\mathcal{F}_i\mathcal{G}_iB - K_iC_iB) = B-KCB$, we conclude that $\widetilde{\mathcal{S}}_j$ satisfies the following recursive equation

$$\widetilde{\mathcal{S}}_j = (A-KCA)\widetilde{\mathcal{S}}_j\mathcal{J} + (B-KCB)Q(\mathcal{G}_jB - \mathbf{1}_nC_jB)^H + \sum_{i=1}^m r_{ij}K_i\mathbf{1}_n^H. \quad (40)$$

Hence, by *Lemma 3*, $\widetilde{\mathcal{S}}_j = P\mathcal{G}_j^H$ for all $j=1,\ldots,m$, which implies that

$$\begin{bmatrix}\mathcal{F}_1 & \cdots & \mathcal{F}_m\end{bmatrix}\widetilde{\mathcal{W}} = P\begin{bmatrix}\mathcal{G}_1^H & \cdots & \mathcal{G}_m^H\end{bmatrix}. \quad (41)$$

On the other hand, according to the result of least square estimation, it is easy to show that the optimal solution of (30) is given by

$$\check{x}(k) = (\mathcal{G}^H \tilde{W}^{-1} \mathcal{G})^{-1} \mathcal{G}^H \widetilde{W}^{-1} \begin{bmatrix} \hat{\zeta}_1(k) \\ \vdots \\ \hat{\zeta}_m(k) \end{bmatrix},$$

where $\mathcal{G}^H = \begin{bmatrix} \mathcal{G}_1^H & \cdots & \mathcal{G}_m^H \end{bmatrix}$. By (41), we have that

$$\mathcal{G}^H \widetilde{W}^{-1} \mathcal{G} = P^{-1} \begin{bmatrix} \mathcal{F}_1 & \cdots & \mathcal{F}_m \end{bmatrix} \mathcal{G} = P^{-1}.$$

Therefore, it can be obtained that

$$\check{x}(k) = \begin{bmatrix} \mathcal{F}_1 & \cdots & \mathcal{F}_m \end{bmatrix} \begin{bmatrix} \hat{\zeta}_1(k) \\ \vdots \\ \hat{\zeta}_m(k) \end{bmatrix} = \hat{x}(k).$$

According to the definition of $\tilde{\epsilon}(k)$, we can get that

$$\begin{bmatrix} \hat{\zeta}_1(k) \\ \vdots \\ \hat{\zeta}_m(k) \end{bmatrix} = \begin{bmatrix} \mathcal{G}_1 \\ \vdots \\ \mathcal{G}_m \end{bmatrix} x(k) - \tilde{\epsilon}(k). \tag{42}$$

From the optimization problem (30) we know that

$$\begin{bmatrix} \hat{\zeta}_1(k) \\ \vdots \\ \hat{\zeta}_m(k) \end{bmatrix} = \begin{bmatrix} \mathcal{G}_1 \\ \vdots \\ \mathcal{G}_m \end{bmatrix} \begin{bmatrix} \mathcal{F}_1 & \cdots & \mathcal{F}_m \end{bmatrix} \begin{bmatrix} \hat{\zeta}_1(k) \\ \vdots \\ \hat{\zeta}_m(k) \end{bmatrix} - \check{\epsilon}(k). \tag{43}$$

From (42) and (43), it follows that

$$\begin{aligned} \check{\epsilon}(k) &= \left(\begin{bmatrix} \mathcal{G}_1 \\ \vdots \\ \mathcal{G}_m \end{bmatrix} \begin{bmatrix} \mathcal{F}_1 & \ldots & \mathcal{F}_m \end{bmatrix} - I \right) \begin{bmatrix} \hat{\zeta}_1(k) \\ \vdots \\ \hat{\zeta}_m(k) \end{bmatrix} \\ &= \left(I - \begin{bmatrix} \mathcal{G}_1 \\ \vdots \\ \mathcal{G}_m \end{bmatrix} \begin{bmatrix} \mathcal{F}_1 & \ldots & \mathcal{F}_m \end{bmatrix} \right) \tilde{\epsilon}(k). \end{aligned}$$

This completes the proof. ■

REFERENCES

[1] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie, and Y. Chen, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1013–1024, 2016.

[2] H. Zhang and J. Wang, "Adaptive sliding-mode observer design for a selective catalytic reduction system of ground-vehicle diesel engines," *IEEE/ASME Transactions on Mechatronics*, vol. 21, no. 4, pp. 2027–2038, 2016.

[3] J. Yan, C.-L. Chen, X.-Y. Luo, X. Yang, C.-C. Hua, and X.-P. Guan, "Distributed formation control for teleoperating cyber-physical system under time delay and actuator saturation constrains," *Information Sciences*, vol. 370, pp. 680–694, 2016.

[4] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno *et al.*, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), IEEE Symposium on*, 2010, pp. 447–462.

[6] T. M. Chen, "Stuxnet, the real start of cyber warfare? [editor's note]," *IEEE Network*, vol. 24, no. 6, pp. 2–3, 2010.

[7] Q. D. Vu, R. Tan, and D. K. Yau, "On applying fault detectors against false data injection attacks in cyber-physical control systems," in *Computer Communications, IEEE INFOCOM-The 35th Annual IEEE International Conference on*, 2016, pp. 1–9.

[8] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems*, 2010.

[9] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE J. Selected Areas in Commun.*, vol. 32, no. 7, pp. 1460–1470, 2014.

[10] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: a system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, 2010.

[11] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Basar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *2013 6th International Symposium on Resilient Control Systems (ISRCS)*, 2013, pp. 54–59.

[12] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Event-triggered output feedback control resilient against jamming attacks and random packet losses," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 270–275, 2015.

[13] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *The 49th IEEE Conference on Decision and Control*, 2010, pp. 5991–5998.

[14] Y. Qi, P. Cheng, L. Shi, and J. Chen, "Event-based attack against remote state estimation," in *The 54th IEEE Conference on Decision and Control*, 2015, pp. 6844–6849.

[15] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1145–1151, 2015.

[16] ——, "False data injection attacks in cyber physical systems," in *First Workshop on Secure Control Systems*, 2010.

[17] ——, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2016.

[18] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[19] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *Proc. ACM/IEEE Int. Conf. Cyber-Physical Systems*, 2014, pp. 163–174.

[20] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, "Attack-resilient state estimation in the presence of noise," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 5827–5832.

[21] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: a satisfiability modulo theory approach," *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 4917–4932, 2017.

[22] Y. Mo and E. Garone, "Secure dynamic state estimation via local estimators," in *The 55th IEEE Conference on Decision and Control*, 2016, pp. 5073–5078.

[23] X. Liu, Y. Mo, and E. Garone, "Secure dynamic state estimation by decomposing kalman filter," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 7351–7356, 2017.

[24] F.L. Lewis and L. Xie and D. Popa, *Optimal and Robust Estimation (Second Edition)*. CRC Press, 2011.

[25] R. Tibshirani, "Regression shrinkage and selection via the lasso," *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 267–288, 1996.

[26] D. Han, Y. Mo, and L. Xie, "Convex optimization based state estimation against sparse integrity attacks," *IEEE Transactions on Automatic Control*, DOI: 10.1109/TAC.2019.2891458, 2019.